ELECTRICAL, ELECTRONICS AND COMMUNICATIONS ENGINEERING

CRT/DET - RISC-V architectures and hardware accelerators to support security in space applications.

Funded By	FONDAZIONE CRT CASSA DI RISPARMIO DI TORINO [P.iva/CF:06655250014] Dipartimento DET
Supervisor	MASERA GUIDO - guido.masera@polito.it
Contact	MARTINA MAURIZIO - maurizio.martina@polito.it MASERA GUIDO - guido.masera@polito.it
Context of the research activity	The research will address the efficient hardware implementations based on RISC-V platforms able to support key security algorithm in space applications. Addressed algorithm are from three domains: quantum key distribution, post-quantum cryptography, and lightweight cryptography. The chosen algorithms will be modified and re-written to exploit different optimizations like parallelization, data reuse, and better memory management.
	RISC-V, an open and extensible instruction set architecture (ISA), has gained significant momentum across a variety of industries, with its potential for customization and calability making it an ideal fit for space exploration and satellite systems. In the three addressed application fields, the research will consist of both design space exploration and implementation. The work will focus on open-source resources as much as possible, leveraging the RISC-V architecture and an open implementation of the chosen application (like Open Quantum Safe for example) to ensure greater flexibility, transparency, and reusability of the results. The three addressed fields are described below. QKD Post-processing ASIP Quantum key distribution allows to securely share encryption keys between two parties, leveraging the principles of quantum mechanics to make eavesdropping detectable. After sharing photons using a quantum channel, the keys are generated by a post processing algorithm, which consists of: 1. Parameter estimation: block size, key rate, security level and robustness are some examples of parameters that must be estimated from the shared data. 2. Sifting: the raw shared data is filtered to eliminate invalid data (for example

Objectives	data sampled with a base different from the one used for the photon generation). 3. Reconciliation: estimates the errors rate and corrects errors in the input sifted codes while minimizing information leakage. For this step, many approaches have been studied, comprising Cascade, Winnow, LDPC, polar, slice and multidimensional reconciliation. 4. Privacy amplification: the reconciled key may be partially exposed to an eavesdropper. Privacy amplification allows to distill a consistent and highly secure key from a partially secure reconciled key using hashing. 5. Channel authentication: ensures the integrity and security of the communication between the two parties. On one hand, it ensures message integrity, on the other hand, it resists man-in-the-middle attacks, ensuring that messages come from the correct nodes. In the literature, many works can be found on the subject, even though most of them focus on a single phase among the previously mentioned ones. The flexibility of the hardware-software co-design allows a broad range of optimizations, exploiting both tightly-coupled and loosely-coupled approaches, and the performance/area/power trade-offs can be studied to obtain an architecture that fits the space sector requirements. PQC security core Post-quantum cryptography provides a new generation of cryptographic algorithms designed to withstand attacks by future quantum computers: • KEMs allow to generate and share a secret key between the two parties. NIST have recently standardised HQC, which differs from the other standard algorithm, Kyber, by being code-based instead of lattice-based. • The shared key is then used with a symmetric algorithm for fast encryption of data blocks. AES-256 is the standard algorithm, approved by NIST and CCSDS, for this kind of operations. • Digital signatures are used to authenticate the communication, ensuring that the sender of the message can be trusted. NIST approved two lattice-based algorithms (Dilithium and FALCON) as well as a stateless hash-based one (SPHINCS+). The combination of these three phases allows for secure satellite communications, ensuring confidentiality, integrity and authenticity even at the post-quantum level. Lattice-based algorithms like Kyber and Dilithium have been extensively studied, and some space-related applications have also been tested. HQC, on the other hand, has been only recently chosen by NIST for standardisation, meaning that less studies have been conducted on it. Additionally, among the candidates for the additional signature schemes, two code-base algorithms can be found, CROSS and LESS. As part of the work, various algorithms can be tested and optimized developing hardware accelerators. Lightweight cryptography on satellite applications In constrained environments like CubeSats, having small and efficient cryptographic algorithms is crucial. The ASCON family has been recently chosen by NIST as the new standard for lightweight cryptography. Even though the algorithm is not safe from quantum attacks, its speed and compactness make it the perfect candidate for every mission where quantum resilience is not mandatory. ASCON can also be improved against side-channel attacks using different techniques like masking and constant-time execution. While ASCON is the first algorithm being chosen by NIST for the standardization, also other algorithms proved to be compact and efficient. For

	this reason, this work may also consider the comparison with other lightweight algorithms. The algorithms can be efficiently optimized with hardware accelerators, allowing to obtain designs focussed more on performance or area/power savings depending on the mission requirements.

Skills and competencies for the development of the activity	In order to effectively contribute to the research activity, the candidate should have a good back ground in the following fields: 1-Digital circuit design 2-ASIC design flow 3-Computer architecture and micro-controllers 4-Firmware development.